AIR WAR COLLEGE

AIR UNIVERSITY

# IMPROVING DCMA'S CYBERSECURITY AWARENESS TRAINING PROGRAM

by

Rolan T. Bangalan, NH-IV, Defense Contract Management Agency

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Chad Dacus

13 February 2018

## DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

## Biography

Rolan Bangalan is assigned to the Air War College, Air University, Maxwell AFB, AL. He enlisted in the US Navy in 1990 and served as an Aviation Structural Mechanic - Hydraulics with Fighter Squadron 24 in support of Operation DESERT STORM.

As a commissioned officer, he has been assigned to Strike Fighter Squadron 136, Amphibious Squadron 5, and Space and Naval Warfare Systems Command.

As a federal employee, he has been assigned to the Joint Special Operations Command, Transportation Security Administration, and Space and Naval Warfare Systems Command, Systems Center Pacific. Currently, he is with the Defense Contract Management Agency, where he is responsible for policies, training, and tools for the Software Acquisition Management (SAM) workforce.

## Abstract

Rogue states and non-state actors have consistently launched cyber-attacks against Department of Defense (DoD) program offices, information systems, networks, and contractor facilities. In response to this, the DoD has made cybersecurity a requirement for all defense acquisition programs. Thus, according to the DoD, cybersecurity must be fully considered and implemented in all phases and aspects of a program's acquisition life cycle. To enforce this obligation on contracting organizations that do business with the DoD, Software Professionals (SPs) from the Defense Contract Management Agency (DCMA) have to be technically proficient to ascertain if the contractors' performance and management systems are in accordance with DoD's cybersecurity requirements. This study will examine, under the FY 18 Air Force Space Command research priority, "Cyber resilience, Cyber Assurance, and the Third Offset," how DCMA can assess the effectiveness of its Cybersecurity Awareness Training (CAT) and will provide recommendations on how to continually improve this training program. As a government agency, DCMA exists to ensure that defense contract requirements are correctly implemented by contractors. Consequently, by failing to address the current cybersecurity knowledge gap of DCMA's Software Professionals, this particular workforce will be unable to positively influence contractor performance, in this case, compliance with governmental cybersecurity requirements, which would ultimately result in mission failure for the Agency.

## Introduction

Since 2006, "the unauthorized access to and installation of malicious software on US government computers have increased by 650 percent".[1] Furthermore, the Department of Homeland Security reported an alarming total of "198 cyber-attacks on critical US infrastructure during 2012 — a 52 percent increase over those that occurred in 2011."[2] With the ever-growing reliance on weapon systems on networks and information systems, the importance of having effective cybersecurity cannot be emphasized any stronger. On November 18, 2013, to buttress the cybersecurity posture of DoD networks and information systems, the DoD announced Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, to supplement the Federal Acquisition Regulation (FAR). DFARS Clause 252.204-7012 requires contractors to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations", to safeguard covered defense information that is processed or stored on contractors' internal information systems or networks.[3] The clause is effective upon contract award, but contractors have until December 31, 2017, to implement NIST SP 800-171.

Initially, the NIST published SP 800-171 security requirements in June 2015. SP 800-171 is a subset of requirements taken directly from the NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", that specifically apply to Controlled Unclassified Information (CUI) shared by the federal government with a nonfederal entity.[4] The controls protect CUI in nonfederal IT systems from unauthorized disclosure. According to the NIST SP 800-171, CUI is "any information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding

information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended".[5] Simply stated, CUI is "information that is sensitive and relevant to the interests of the United States, but not strictly regulated by the Federal government".[6] CUI encompasses web and electronic mail services, credit card and other financial data, healthcare data, background investigative data for security clearances, data required to provide cloud services, and data associated with developing communications, satellite, and weapons systems.[7]

Evidently, the controls specified in SP 800-171 are meant as guidelines to successfully address compliance with the CIA (confidentiality, integrity, and availability) triad. Thus, safeguards must exist to counter possible threats to the confidentiality, integrity, and availability of CUI and the systems that permit access to it. The CIA triad is the three main principles which guarantee the security of an information system. Confidentiality certifies that "the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure".[8] While integrity is maintained "when the assurance of the accuracy and reliability of information and systems is provided and any unauthorized modification is prevented".[9] Whereas, availability guarantees "reliability and timely access to data and resources" to authorize processes.[10]

Accordingly, contractors who need access to CUI must implement and verify compliance and create security protocols for fourteen key areas. Per the SP 800-171, the fourteen families of security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations include

- Access Control – Who is authorized to view data?
- Awareness and Training – Are contractor personnel properly trained to treat CUI?

- Audit and Accountability – Are records appropriately maintained?
- Configuration Management – Are security protocols configured and documented?
- Identification and Authentication – Are users verified before given access to CUI?
- Incident Response – Are processes in place to cope with a security breach?
- Maintenance – Are maintenance responsibilities delineated?
- Media Protection – How secure are electronic and hard copy records?
- Personnel Security – How well is the screening process for personnel who need access to CUI?
- Physical Protection – Is access to systems and storage environments controlled?
- Risk Assessment – Are operations or individuals verified consistently?
- Security Assessment – Are current processes and procedures still effective?
- System and Communications Protection – Is data regularly monitored and controlled at key internal and external transmission points?
- System and Information Integrity – How quickly are possible threats detected, identified and corrected? [11]

To document implementation of the SP 800-171 security requirements, contracting companies should have a system security plan in place, "in addition to any associated plans of action to describe how and when any unimplemented security requirements will be met, how any planned mitigations will be implemented, and how and when they will correct deficiencies and reduce or eliminate vulnerabilities in the systems."[12]

Truly, cybersecurity has exponentially grown in importance for the DoD as "nearly 100 percent of day-to-day operations are completed on some type of information system".[13] Recently, at a Senate Select Committee on Intelligence hearing held on February 13, 2018, the Director of

National Intelligence stated that because of the growth of the growth of the cyber domain and America's increasing vulnerability, cyber tops the list of threats to the US.[14] As a DoD component, DCMA needs to contribute to improving the country's posture with regard to cybersecurity. In its pursuit of ensuring that cybersecurity requirements are sufficiently executed by defense contractors, DCMA fulfills one of its software acquisition mission by safeguarding CUI in nonfederal IT systems.

In this study, the research problem that will be explored is "How to continually improve DCMA's Cybersecurity Awareness Training in order to eliminate the cybersecurity knowledge gap of DCMA's Software Professionals?" To address this question data from an online survey on SPs who have completed DCMA's Cybersecurity Awareness Training will be examined to evaluate the effectiveness of this training program. By using data from this online survey, the following metrics will be taken to gauge progress and impact:

Reaction: How did the SPs respond to the training program?

Learning: Did the training improve the SPs' knowledge and skills?

Behavior: Did the SPs' behavior change positively as a result of the training?

**Improving DCMA's Cybersecurity Awareness Training Program**

*It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. We're not as prepared as we should be, as a government or as a country.*

– President Barack Obama

Within the DoD, DCMA, an independent combat support agency, has been promptly making preparations for the implementation of DFARS Clause 252.204-7012. As DoD's contract manager, DCMA strives to be the "independent eyes and ears of DoD and its partners, delivering actionable acquisition insight from the factory floor to the front line … around the world."[15] As the DoD's watchdog on contractual compliance on software requirements, DCMA recently evaluated the technical competence of its SP personnel to assess the readiness of this workforce in administering DFARS Clause 252.204-7012.

While SPs have been entrusted with DCMA's Software Acquisition Management (SAM) mission, they are not part of DoD's Information Assurance (IA) workforce. Hence, these employees are not subject to the stringent requirements stipulated in DoD Directive 8570.01-M Manual Information Assurance Workforce Improvement Program. However, they own the responsibility of ensuring that DoD "customers receive software products and/or systems with embedded software that meet or exceed contractual specifications/requirements, and provide our customers with the knowledge to allow them to make informed milestone and other on-going decisions relative to software cost, schedule, and technical performance."[16] Consequently, it is imperative that SPs attain a certain level of cybersecurity technical competency to enforce properly DFARS Clause 252.204-7012.

The Federal Information Security Modernization Act (FISMA) of 2014 specifically requires that the heads of all federal agencies, ensure that all users are held accountable for their responsibilities in complying with agency policies concerning information security risks associated with their activities. In addition to the FISMA, DoD agencies have to comply with DoD Instruction 8500.01, "Cybersecurity," dated March 14, 2014. DoD requires its components to provide additional cybersecurity orientation, training, and awareness programs to reinforce the objectives of the DoD Enterprise cybersecurity awareness programs to authorized users of information systems (IS). To comply with both, IS users have to complete the mandatory DoD Cyber Awareness Challenge annually. In addition to providing baseline knowledge in cybersecurity, the objectives of the DoD Cyber Awareness Challenge include

- enhancing the physical security of computer hardware and software
- limiting access to computer equipment to authorized users only
- preventing computer fraud, waste, and abuse
- implementing effective contingency planning
- prompt reporting of security problems to the chain of command
- protecting computer files from infection by malicious logic[17]

Annual security awareness training, like the DoD Cyber Awareness Challenge, helps employees to recognize and respond to threats. This not only reduces the number of threats that are prevented before materializing, but it also reduces the damage done by any undetected threat in terms of data losses, downtime, or other interruptions caused by an attack or another incident.

Unquestionably, the DoD Cyber Awareness Challenge suitably emphasizes cyber hygiene techniques, i.e., how to stay safe from phishing attacks, how to keep your email safe, and how to properly configure a wireless network.[18] However, it is still woefully inadequate in

providing the knowledge required by SPs when performing contract surveillance on a software project. Per the NIST SP 800-171, in order to effectively protect information system resources, contractors are required to have a system security plan. Thus, when DFARS Clause 252.204-7012 takes effect, SPs will have to ascertain if a contractor has a documented system security plan. As pointed out, the DoD Cyber Awareness Challenge falls short in providing the knowledge required by the SPs to execute their tasks effectively.

Accordingly, DCMA focused on the need to fill this training gap. Thus, in January 2017, the Software Division of DCMA's Technical Directorate established a cybersecurity working group to ascertain cybersecurity contractual requirements that SPs will have to incorporate in their contract surveillance plans. Since the existing training program of the SPs, the Software Professional Development Program (SPDP), centers exclusively on software development activities, the cybersecurity working group was also assigned to formulate a training plan that will supplement SPDP which will augment cybersecurity knowledge into their surveillance skillset. The working group was composed of several cybersecurity subject matter experts (SMEs) from the Software Division and representatives from field offices where contract surveillance is actually performed. The virtual weekly meetings held by the cybersecurity working group were open, which allowed any SP to listen in and to provide inputs.

## Survey of Training Methodologies

A training methodology, also known as an instructional design model, is used to outline the events that will steer the development of eLearning projects. It allows training developers to convey the objective and reason behind a chosen strategy. Thus, a training methodology is a framework that offers a high-level perspective of all the main components that have to be

included in the training program.[19] The following are the most widely used methodologies that training developers use to structure and plan their eLearning courses:

**ADDIE**

The ADDIE model, widely used for designing and developing training programs, is an "adaptation of the systems engineering process to problems of workplace training and instruction."[20] ADDIE stands for Analysis, Design, Development, Implementation, and Evaluation. The ADDIE model process assumes that "alternative solutions to instructional problems will be more or less cost-efficient depending on the instructional need and environmental constraints and that using a systems approach intelligently to choose among alternative solutions will produce the most effective results."[21] Analogous to the waterfall model of software development, the ADDIE model prescribes following a repeatable series of steps, fine-tuned for the scope and context of the project in order to drive speed and quality. When the ADDIE process was initially specified, it represented the then prevailing specification for the design and development of systematic training utilized in a military environment of imparting the skills for highly specified job tasks by a continuous stream of homogeneous learners.[22]

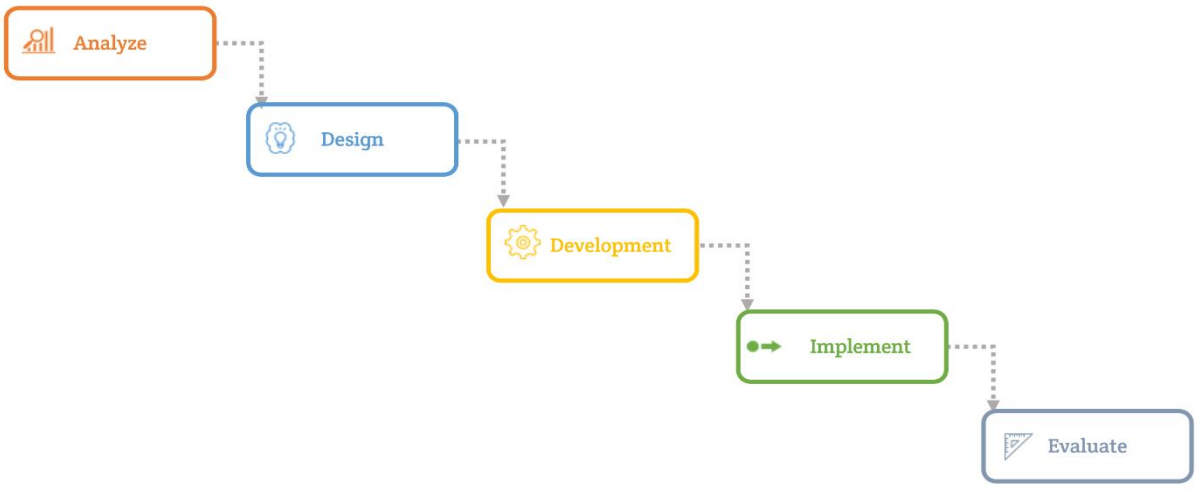


*Figure 1.* ADDIE Process[23]

**AGILE**

The AGILE Learning Design, an iterative model of instructional design, focuses on collaboration and rapid prototyping. According to its proponents, AGILE is "the new alternative to the old – and some have argued outdated – ADDIE model."[24] Introduced by Conrad Gottfredson, the AGILE design approach is a project-oriented approach which encompasses the five stages involved when designing eLearning courses: Align, Get set, Iterate and implement, Leverage, and Evaluate.[25] AGILE allows the insertion of new technologies and more rapidly evolving ideas; it permits adjustment on the fly, the demonstration of mockups, prototypes, and early suggestions with the end users. By using AGILE, the end users can provide feedback during the development of the training. Notably, proponents of AGILE tout its greatest benefit, its ability to produces quality eLearning courses more rapidly.[26]

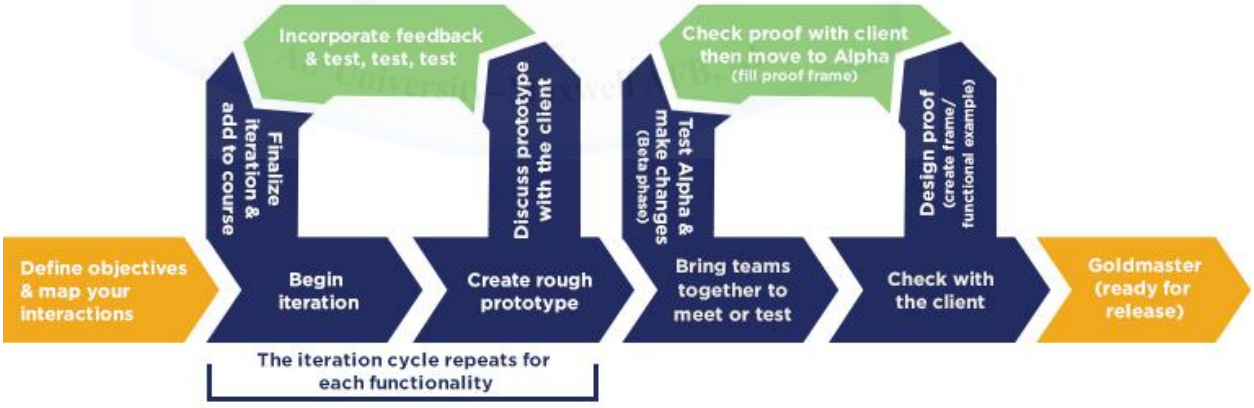


*Figure 2.* AGILE Learning Design Process[27]

**Successive Approximation Model (SAM)**

According to its creator, Michael Allen, SAM provides "a clear pathway to success, measurable and obtainable milestones for marking completion, and targeted moments to reach agreement and consensus".[28] SAM's most prominent feature is that it offers the training

developers opportunities to make changes by executing small steps and multiple iterations. SAM begins with a brief Preparation phase, where material for the eLearning project is collected.[29] Afterwards, the project moves to the Iterative Design and Iterative Development where the design is generated and appraised.[30] Because this training methodology consists of repeated small steps or iterations, SAM provides a design approach that addresses most of the usual instructional design pain points, i.e., meeting deadlines, keeping on budget, and working with SMEs.[31]


*Figure 3.* SAM Process[32]



## Cybersecurity Awareness Training Program

After the formation of the cybersecurity working group in DCMA's Technical Directorate, the working group members began developing DCMA's Cybersecurity Awareness Training (CAT) Program (see appendix A). The first task was to select the methodology to develop the training program. Even though critics of ADDIE point out that its biggest weakness is that "it assumes that developers know all of the training requirements before the content is developed".[33] Unanimously, the cybersecurity working group chose the ADDIE model as the framework for the proposed cybersecurity training. The working group members preferred ADDIE's benefit of offering "a dynamic, flexible guideline for building effective training and

performance support tools".[34] Moreover, ADDIE's ongoing feedback throughout all its phases allows design flaws to be recognized while they are still easy to fix.[35]

By using the ADDIE methodology, a cybersecurity knowledge gap within the SP ranks was discovered during the Analyze phase. Even after completing the mandatory DoD Cyber Awareness Challenge, SPs still require additional cyber knowledge in order to perform their duties proficiently.

Faced with the constraint of diminishing training funds, DCMA's cybersecurity working group made a deliberate effort during the Design and Develop phases to come up with a cost-effective means to train the SP workforce. Because of fiscal constraints, the cybersecurity working group leveraged existing online courses provided for free by the Defense Acquisition University (DAU), Department of Homeland Security's (DHS) Federal Virtual Training Environment (FedVTE), and Defense Security Service's (DSS) Center for Development of Security Excellence (CDSE). From these free resources, members of the cybersecurity working group registered and completed each training module. Upon completion of all the modules, the cybersecurity working group evaluated these modules for relevance and applicability to the prospective Cybersecurity Awareness Training. The evaluation resulted in the exclusion of unnecessary courses. While appropriate modules were selected to comprise the Cybersecurity Awareness Training, which will eventually address the SPs' cybersecurity knowledge gap.

Then, in the Implement phase, required announcements, instructions, and various administrative functions were completed in order to launch the training. In the future, when there is a sizable number of graduates, the CAT will enter the Evaluate phase. During this phase, the working group members will determine the effectivity of the CAT. It should be noted that even though this is the last phase of the ADDIE model, evaluation has to take place throughout each

phase of the training process, not as the last step. At the Evaluate phase, the training program is continuously monitored. Feedback has to be obtained from training participants to determine the training program's effectiveness and to identify any weaknesses. By sustaining a continuous feedback loop, the quality and relevance of the training material will be maintained. Moreover, doing this will allow for a suitable action plan to be created in order to address the identified deficiencies.

**Advantages and Disadvantages of Using Surveys**

Conducting an informal survey offers the following advantages:

- Cost-efficiency – Online surveys incur a negligible cost per participant as resources, such as a computer and network connectivity, are readily available.[36]
- Ease of Data Collection – Surveys done online facilitates data compilation and analysis.[37]
- Sample Size – Hosting the survey on DCMA's website offers scalability and allows reaching out to scores of possible participants. This advantage will ensure a more accurate sample from which to draw conclusions.
- Candid Responses – Completion of the survey will be done anonymously to allow graduates to feel more candid with their responses. By letting respondents be as honest as possible with their answers will yield more reliable data.[38]

However, informal surveys also suffer from shortfalls. These disadvantages include:

- Inflexible Design – After the survey is developed, the method of administering it, along with the survey questions, cannot be changed during data collection.[39]

- The absence of an interviewer – If respondents are willing to share more details on their answers, not having an interviewer to capture this information or probe for more particulars will somehow affect data analysis.[40]

In spite of these disadvantages, the feedback gathered from the survey will be critical in improving DCMA's Cybersecurity Awareness Training. Consequently, it will be relatively easy to determine if the SPs are taking the newly-gained knowledge and skills from the training and applying them where they count.

**Evaluating Effectiveness**

As in all endeavors, progress cannot be considered until after an objective review and a full analysis of the results are performed.[41] Thus, in order to assess the effectiveness of Cybersecurity Awareness Training program, a method of tracking progress and appraising impact has to be instituted. According to the NIST, "metrics monitor the accomplishment of the awareness and training program goals and objectives by quantifying the level of implementation of awareness and training and the effectiveness and efficiency of the awareness and training, analyzing the adequacy of awareness and training efforts, and identifying possible improvements".[42] Remarkably, gauging the effectiveness of an awareness program can be challenging.[43] Since metrics show progress and impact to the organization, training developers use these metrics "as a guide for making adjustments to the program and reporting progress to senior management".[44] To evaluate the effectiveness of an awareness program, the NIST recommends the following metrics: "percentage of users completing required awareness session or exposure and percentage of users with significant security responsibilities who have been trained in role-specific material".[45] For DCMA, the following metrics will be used:

Reaction: How did the SPs respond to the training program?

Learning: Did the training improve the SPs' knowledge and skills?

Behavior: Did the SPs' behavior change positively as a result of the training?

## Lessons Learned and Best Practices from External Organizations

DCMA's cybersecurity working group purposefully chose the ADDIE model to take advantage of its primary feature, that of allowing iterative improvements to a training program. Since this study attempts to extract best practices and lessons learned from outside organizations, DCMA's Cybersecurity Awareness Training will be enriched by incorporation of innovative techniques. The following organizations have been researched about their homegrown cybersecurity awareness programs.

### Application Software Assurance Center of Excellence (ASACoE)

Located at Maxwell Air Force Base, the Air Force's Application Software Assurance Center of Excellence stood up in 2007.[46] Following an embarrassing exploitation of an Air Force information system, ASACoE was launched to "raise awareness about the criticality of application security, implement Web- and database-level application monitoring, and train and mentor software developers to identify and repair existing software vulnerabilities and/or incorporate security into coding practices".[47] ASACoE has "trained 332 personnel, identified more than 750,000 weaknesses in 190 applications, provided fixes for more than 200,000 of them, and helped to eliminate or mitigate 25 of the most serious application vulnerabilities".[48] According to Maj. Michael Kleffman, ASACoE's Chief Technology Officer, the center's mission "is to foster security in every step of the software development lifecycle (SDLC) and in software acquisitions through tools, techniques, and education".[49] ASACoE partners "with the acquisition community to educate it about software assurance and to better understand the

importance of including software assurance in software acquisitions".[50] Upon request, the ASACoE team provides program offices with software development training. The training includes secure software development, the vulnerabilities of programming languages, the use of a source code analysis tool, the use of a database analysis tool to analyze database configuration, and a brief of the management and shielding tools.[51] By fostering security into the software development lifecycle (SDLC) and software acquisitions through techniques, tools, and education, ASACoE has leveraged information technology through the deployment of practices and automated tools that supported and imid Air Force software development processes.[52] Throughout the establishment of the center, selecting its tools, instructing developers, and evaluating and repairing databases and applications, ASACoE has identified a number of lessons learned, such as:

1. realizing that security is an unceasing activity that must be continuously addressed and readdressed[53]
2. having an active awareness campaign that reminds program and acquisition managers of the security risks[54]
3. all echelons of management, to include the program manager, should grasp the significance of software assurance and be ready to shoulder the extra upfront expenses of integrating software assurance in the SDLC; by instilling software assurance from the start, management will realize cost savings as software weaknesses are corrected earlier in the development lifecycle[55]
4. education is critical in forming a rigorous software-assurance framework in any organization[56]

Truthfully, ASACoE, with its wealth of knowledge in implementing software security and preventing compromises in software applications, would have been a great resource that DCMA could have used to further its quest of improving its CAT program. However, lack of funding caused the disbandment of ASACoE in 2015.[57]

**Defense Information Systems Agency (DISA)**

The ballooning volume of network breaches, the increasing sophistication of cyber-attacks, and the advancing talents of adversaries are among the cybersecurity challenges that are of utmost importance to Roger Greenwell, DISA's Chief of Cybersecurity.[58] So, to keep up with evolving cyber threats, DISA's training tactics have also changed. Greenwell acknowledges that training lays the foundation for successful cybersecurity in any organization.[59] Charged with cybersecurity training for the Defense Department, DISA is revamping its approach by emphasizing continual training.[60] Recognizing that taking an annual course and completing its test is inadequate, DISA has embarked on delivering smaller sessions of more frequent training. For this reason, in 2015 DISA created Cyber Defender to provide continual cybersecurity awareness through virtual learning questions, tips, interactive videos, and referential cybersecurity material. Cyber Defender is used to prepare the DISA authorized users against the evolving cyber threat landscape.[61] Weekly, the Cyber Defender tool delivers new training information that addresses emerging cyber trends, threats, and issues that affect the workforce at the Defense Information Systems Agency.[62] The program consists of virtual learning questions, tips, and interactive videos to supplement the annual DoD Cyber Awareness Challenge.

On a pre-determined workday, Cyber Defender presents a short quiz to a computer user after a successful log-in. The cybersecurity questions vary from week to week. If a user answers questions carelessly or incorrectly will land that user some additional reading to brush up on the

topic.[63] Currently, DISA's question bank includes over 64 questions covering topics such as Phishing, Credentials/Passwords, Acceptable Use, Email, Emerging Threats, Social Networking, Mobile Devices, Physical Security, Removable Media, Insider Threat, and Personally Identifiable Information (PII).[64]

By providing a constant reminder, DISA ensures that its workforce is thinking about cybersecurity every week.[65] According to Cyber Defender's Program Manager, Tiffiney Benton, her most important lesson learned is to make participation in Cyber Defender's mandatory to increase the current 40% voluntary participation. Additionally, she plans to acquire a COTS product for improved capability, to increase question types, and to add scenario-based options and videos.[66]

**Symantec**

Headquartered in Mountain View, California, Symantec provides cybersecurity software and services. For a fee, Symantec offers its Security Awareness Service, video-based educational courses, to customers who need to meet industry-related compliance mandates, as well as the security standards required for certain positions within an organization. According to Symantec, its Security Awareness modules cover key training required by every employee at every level of an organization. Its video modules include 1) Acceptable Use, 2) Phishing, 3)Passwords, 4) Privacy, 5) Insider Threats, 6) Access Control and Provisioning, 7) Media Handling, 8) Information Security for Program Management, 9) Information Security Program for IT Security, 10) Vulnerabilities, Threats, and Controls, 11) Payment Card Industry Data Security Standard (PCI DSS), 12) HIPAA and HITECH, 13) Data Protection and Destruction, 14) Working Remotely, 15) Physical Security, 16) Backups, 17) SDLC Security Awareness, 18) System Policies, 19) Securing Network Communications, 20) Partnering with the Information

Security Department, 21) The Role of the Help Desk in an InfoSec Program, 22) Network Security Overview, 23) Information Security Risk Basics, 24) Information Security Risk Management, 25) Audit Overview, 26) Information Security Roles, 27) Overview of Operational Security, 28) Contracting and System Acquisition, and 29) Disaster Recovery and Business Continuity. In the future, Symantec will release the following modules: Internet of Things (IoT), General Data Protection Regulation (GDPR), Cloud Access Awareness, and Ransomware.[67]

Additionally, Symantec introduced a capability that would allow any organization the ability to carry out simulated phishing attacks on its employees.[68] Symantec's Phishing Readiness gives organizations the ability to deploy targeted emails and to keep track of how well employees recognize a phishing attack.[69] Upon failing a test, an employee is forced to take a remedial cybersecurity training on the spot.[70] Symantec maintains that its Security Awareness Service promotes proactive employee behavior to protect information better and helps decrease the risk of loss of vital data.[71]



## Recommendations

During a preliminary review of the completed forms to the CAT completion survey, participants gave high marks to the adequacy and relevance of the training modules. Additionally, the three responding participants claimed that there was a significant increase in cybersecurity knowledge that they could apply in the execution of their surveillance duties. Although, all three acknowledging participants complained about the lengthiness and the excessive time expended to complete some of the modules.

From the SP population of 500, choosing a 90% confidence level and a 10% margin of error yields a sample size of 60 (see appendix B). Since only 22 SPs have completed the CAT as of December 2017 and only three have completed the survey,[72] performing an analysis will be

premature. As the sample size determines the level of confidence, attempting to draw a precise and accurate conclusion from an inappropriate sample size will surely provide an invariably inconclusive result.[73] Hence, before conclusions are drawn from the review of collected feedback for the CAT, the sample size has to be at least equal to or greater than 60.

In light of the preceding information presented, the following are the recommendations that have to be implemented in order to improve DCMA's Cybersecurity Awareness Training program:

1. *Continuously review data results from training feedback surveys*. In order to be effective at their jobs, SPs have to be properly trained. Thus, the Cybersecurity Awareness Training program has to be relevant and flexible at all times. Relevance will ensure that superfluous information will be deleted from the program; flexibility will guarantee that changes to the FAR and DFARS will be reflected almost instantaneously in corresponding changes to the training modules. Furthermore, in order to effectively assess the CAT, SPs have to be exhorted to complete the training program and the corresponding training feedback survey. The Software Division, as the responsible organization, has to devote the requisite manpower and resources to this end.
2. *Constantly monitor external agencies for innovative and cost-effective Cybersecurity Awareness programs*. In today's fiscally-constrained environment, training dollars are hard to come by. Thus, it is advantageous to assess training programs developed by outside agencies for best practices and lessons learned. After such an assessment, if a program is found to be applicable and relevant to the needs of the SPs, then arrangements should be made for its incorporation into DCMA's CAT. From DISA and Symantec, the recurring theme was that mandatory smaller sessions of frequent training are more

effective in improving awareness. With regard to this particular lesson learned, the Software Division, as the responsible organization, has to investigate the feasibility of making the CAT compulsory and offering CAT sessions in smaller chunks on a recurring basis.

## Conclusion

As the DoD evolves from the industrial age to the information age, correcting cybersecurity weaknesses and maintaining adequate cybersecurity takes more importance.[74] Imperatively, for DCMA, its Cybersecurity Awareness Training Program has to effectively train SPs in order to fulfill its Software Acquisition Management mission. While DCMA strives to continuously improve, the SPs within the Software Division are presently in a state of transition as they prepare to meet the future challenges of administering DFARS Clause 252.204-7012. With this transition comes the requirement for training agility and adaptability necessary for SPs in order to execute their tasks effectively. The difficulty of operating in an environment characterized by an enormous flow of information and constant change will become more manageable with employment of learning science, experience, and the application of realistic training. Furthermore, stuck in a resource-constrained environment, fulfilling the SP workforce's training needs to equip them in their future enforcement of DFARS Clause 252.204-7012 will definitely be challenging.

# Appendix A

## Cybersecurity Awareness Training Program Guide[75]

Cybersecurity Awareness Training Program Guide, March 2017

**Table of Contents**

## 1. Program Overview

The Software Division's Cybersecurity Awareness Training Program is not a mandatory requirement. However, all individuals, regardless of their job series, who are supporting Software Acquisition Management (SAM) within the Agency, are highly encouraged to participate in the Cybersecurity Awareness Training Program. The goals of the Cybersecurity Awareness Training Program are 1) to aid Software Professionals (SP) in the attainment of the Defense Acquisition Workforce Improvement Act's (DAWIA) requirement of 80 Continuous Learning Points every two years and 2) to educate Software Professionals about common cybersecurity concepts and enhance the understanding of the threats and challenges faced by the Department of Defense.

## 2. Cybersecurity Awareness Training Program Certification Requirements

To complete the Cybersecurity Awareness Training Program, the trainee has to complete a minimum of 40 hours in training that includes the three DAU core courses. Table 1 lists the online courses that the trainee can choose from to accumulate the required 40 hours.

| **DAU Courses (Core Courses)** |
|---|
| ACQ 160 Protection Planning Awareness |
| CLE 074 Cybersecurity throughout DoD Acquisition |
| CLE 075 Introduction to DoD Cloud Computing |
| **CDSE Courses (Core+ Courses)** |
| Introduction to the NISP Certification and Accreditation Process (IS100.16) |
| Risk Management Framework (RMF) Step 1: Categorization of the System (CS102.16) |
| Risk Management Framework (RMF) Step 2: Selecting Security Controls (CS103.16) |
| Risk Management Framework (RMF) Step 3: Implementing Security Controls (CS104.16) |
| Risk Management Framework (RMF) Step 4: Assessing Security Controls (CS105.16) |
| Risk Management Framework (RMF) Step 5: Authorizing Systems (CS106.16) |
| Risk Management Framework (RMF) Step 6: Monitor Security Controls (CS107.16) |
| Acquisition and Contracting Basics in the NISP (IS123.16) |
| **FedVTE Courses (Core+ Courses)** |
| Continuous Diagnostics and Mitigation (CDM) Module 1 : Overview |
| Continuous Diagnostics and Mitigation (CDM) Module 2: Hardware Asset Management |
| Continuous Diagnostics and Mitigation (CDM) Module 3: Software Asset Management |
| Continuous Diagnostics and Mitigation (CDM) Module 4: Configuration Settings Management |
| Continuous Diagnostics and Mitigation (CDM) Module 5: Vulnerability Management |
| Cyber Risk Management for Managers |
| Cyber Security Overview for Managers |
| DNSSEC Training Workshop |
| Introduction to Investigation of Digital Assets |
| Introduction to Windows Scripting |
| LAN Security Using Switch Features |
| Network Layer 1 & 2 Troubleshooting |
| Radio Frequency Identification (RFID) Security |
| Securing Infrastructure Devices |

*Table 1.* Cybersecurity Courses

## 3. Procedure for Requesting the Cybersecurity Shield of Excellence Certificate

a. Once a trainee accumulates 40 hours of training from the courses listed in Table 1, said trainee is eligible to receive the Software Division's Cybersecurity Shield of Excellence Certificate. The trainee will send a completed request to the Software Division Training Lead along with the substantiating certificates of completion.

b. Upon receipt of the request, the Software Division Training Lead will review the submitted package to ensure that the individual meets the certification criteria.

c. If all requirements have been met, the Software Division Training Lead will provide a scanned copy of the Software Division's Cybersecurity Shield of Excellence Certificate to the trainee. A formal certificate will be generated by the Software Division, signed by the Software Division Director and will be sent to the CMO Commander for presentation to the trainee.

d. For disapproved requests, the Software Division Training Lead will notify the trainee and the trainee's immediate supervisor of the reason for disapproval via email.

## Appendix A. Cybersecurity Awareness Training Program Responsibilities

**A-100 PURPOSE:** To establish responsibilities related to the Cybersecurity Awareness Training Program.

**A-101 Trainees are responsible for:**

a. Reviewing and discussing Cybersecurity Awareness Training Program requirements and status with trainee's immediate supervisor.

b. Ensuring the Learning Map is updated in TMS as necessary.

c. Providing verifiable evidence of completion of online training through trainee's immediate supervisor for entry into trainee's training records.

d. Submitting a Cybersecurity Shield of Excellence Certificate request through trainee's chain of command after all program requirements have been completed.

e. Ensuring every effort is made to satisfactorily complete all required Cybersecurity classes in a timely manner.

**A-102 Supervisors are responsible for:**

a. Encouraging subordinate Software Professionals to pursue Cybersecurity Awareness Training Program.

b. Ensuring that the Learning Map for each trainee is updated to reflect required Cybersecurity Awareness Training Program courses.

c. Reviewing and approving requests for Cybersecurity Shield of Excellence Certificate in a timely manner.

**A-103 Software Division Director is responsible for**:

a. Providing strategic direction regarding the management of the Cybersecurity Awareness Training Program.

b. Signing Cybersecurity Shield of Excellence Certificates and congratulatory letters.

c. Representing this program, as needed, to the Agency Senior Leader Team (SLT).

**A-104 Workforce Development is responsible for**:

a. Working with the Software Division Training Lead to establish Cybersecurity Awareness Training Program courses in TMS.

**A-105 Software Division Training Lead is responsible for:**

a. Serving as technical advisor and training lead for the Cybersecurity Awareness Training Program.

b. Evaluating the effectiveness of the subject courses.

c. Revising and updating policy related to Cybersecurity Awareness Training Program.

d. Maintaining the Cybersecurity Awareness Training Program Database.

e. Reviewing and dispositioning requests for Cybersecurity Shield of Excellence Certificate.

f. Preparing Cybersecurity Shield of Excellence Certificates for presentation to the recipients once requirements have been completed.

g. Coordinating with Workforce Development in establishing Cybersecurity Awareness Training Program courses in TMS.

## Appendix B. Course Descriptions

The following is a list of courses and their descriptions that are available to the trainee. [Note that in order to take these courses, a student has to register at the appropriate website. Follow these hyperlinks to get to the registration site: Defense Acquisition University (https://www.dau.mil/), Center for Development of Security Excellence (http://www.cdse.edu/stepp/index.html), Federal Virtual Training Environment (https://fedvte.usalearning.gov/)]

| **ACQ 160** |
|---|
| **Program Protection Planning Awareness** |
| **SOURCE:** Defense Acquisition University |
| **TMS CODE:** N/A |
| **LOCATION:** Defense Acquisition University Distance Learning |
| **LENGTH:** 17 hours. This is a nonresident, self-paced course available on-line. Trainees must pass the final examination within 60 calendar days of the start date. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to: recognize system security threats and consequences to acquisition programs and that the system security solution approach includes risk-based prevention, detection, and response to system security threats; define critical program information (CPI), CPI policy, CPI threat definition, and associated attacks; identify trusted system and network threat definitions, associated attacks, and policy; recognize the requirement of the Program Protection Plan (PPP) within the Acquisition Life Cycle and how program protection is incorporated into the Request for Proposal (RFP); define the roles and responsibilities of the program manager (PM), systems engineer (SE), system security engineer (SSE), system security engineering specialists, security specialists, chief developmental tester, and the contractor with respect to system security; recognize how program protection integrates system security engineering specialties and security specialties through a high level overview of each specialty's activities and outputs; relate the protection measure and mitigation steps to specific acquisition solicitations scenarios. |
| **DESCRIPTION:** This course emphasizes the principles and policies of system security engineering. Program protection planning requires each acquisition's integrated product team to prevent, detect, and respond to program protection challenges. This course provides training on threats, vulnerabilities, risks, cost-benefit risk trade-offs, and required mitigations for DoD systems. It also addresses supply chain management and the need for acquisition program protection documents such as the Program Protection Plan, Cybersecurity Strategy, and security plans. |
| **CONTINUOUS LEARNING POINTS:** 17 |
| **DAI:** Process code: IHC04 - Training |

| CLE 074 |
| --- |
| **Cybersecurity Throughout DoD Acquisition** |
| **SOURCE:** Defense Acquisition University, Continuous Learning |
| **TMS CODE:** N/A |
| **LOCATION:** Defense Acquisition University Distance Learning |
| **LENGTH:** 5 hrs. This is a nonresident, self-paced course available on-line. Trainees must pass the final examination within 60 calendar days of the start date. |
| **OBJECTIVES:** See DAU icatalog, http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=2048 |
| **DESCRIPTION:** This continuous learning module provides foundational understanding of basic principles of cybersecurity and cybersecurity risk management in the defense acquisition field. |
| **CONTINUOUS LEARNING POINTS:** 5 |
| **COURSE COMPLETION REQUIREMENTS:** Completion of an end-of-module test with a 100% score |
| **DAI:** Process code: IHC04 - Training |



| CLE 075 |
| --- |
| **Introduction to DoD Cloud Computing** |
| **SOURCE:** Defense Acquisition University, Continuous Learning |
| **TMS CODE:** N/A |
| **LOCATION:** Defense Acquisition University Distance Learning |
| **LENGTH:** 4 hrs. This is a nonresident, self-paced course available on-line. Trainees must pass the final examination within 60 calendar days of the start date. |
| **OBJECTIVES:** See DAU icatalog, http://icatalog.dau.mil/onlinecatalog/courses.aspx?crs_id=2117 |
| **DESCRIPTION:** This continuous learning module will explain what cloud computing is and how cloud services work so that you can recognize the benefits and risks to the DoD and your Component. In addition, the CLM will discuss the activities a DoD organization would need to observe in order to use a commercial cloud service offering (CSO) and some of the legal and cybersecurity concerns you should be aware of when choosing the CSO. |
| **CONTINUOUS LEARNING POINTS:** 4 |

| |
|---|
| **COURSE COMPLETION REQUIREMENTS**: Completion of an end-of-module test with a 100% score |
| **DAI:** Process code: IHC04 - Training |
| **IS100.16** |
| **Introduction to the NISP Certification and Accreditation Process** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 2 hours. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br><br>• Define C&A and the purpose of certifying and accrediting contractor information technology systems<br>• Identify the legal, regulatory, and contractual requirements that govern the certification and accreditation process<br>• Identify and define the government and contractor roles and responsibilities related to the C&A Process<br>• Identify and define the components of the Risk Management Process<br>• Identify key sources of risk<br>• Identify and define security objectives, protection levels, and the need-to-know basis for confidentiality<br>• Identify the relationship between system interconnection, information sharing, and securing classified information |
| **DESCRIPTION:** This course introduces the NISP Certification and Accreditation (C&A) Process. The course provides training on the policies and standards used to protect information within computer systems in support of the DSS mission. In addition, the course identifies and defines the government and contractor roles and responsibilities. It also includes the Risk Management Process as it relates to the C&A Process. |
| **COURSE PREREQUISITE(S):** None |
| **COURSE COMPLETION REQUIREMENTS**: Completion of an end-of-module test with a 75% score. |
| **DAI:** Process Code: IHC04 - Training |

| CS102.16 |
| --- |
| **Risk Management Framework (RMF) Step 1: Categorization of the System** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 0.6 hr. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br><br>• Identify security categorization resources<br>• Define security categorization<br>• Identify roles and responsibilities for Step 1<br>• Identify information types<br>• Define impact values and their application<br>• Describe confidentiality security categorization factors<br>• Define system boundaries and be prepared to complete the Security Plan<br>• Complete registration of the information system |
| **DESCRIPTION:** This course covers the first step of the Risk Management Framework (RMF) process: Categorization of the System. Upon completion, students will understand how to determine and apply the appropriate security requirements for an information system prior to registration. This course also discusses the roles and responsibilities related to system categorization and security plan preparation. |
| **COURSE PREREQUISITE(S):** None |
| **DAI:** Process Code: IHC04 - Training |

| CS103.16 |
| --- |
| **Risk Management Framework (RMF) Step 2: Selecting Security Controls** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 0.5 hr. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br><br>• Define security control policies and guidelines<br>• Identify security controls and common controls<br>• Describe and select security controls<br>• Describe the purpose of security overlays and tailoring<br>• Explain the importance of continuous monitoring<br>• Indicate who approves the security plan<br>• Explain when to update the security plan |
| **DESCRIPTION:** This course covers the second step of the Risk Management Framework (RMF) process: Selecting Security Controls. Upon completion, students will be able to select and implement an appropriate initial set of security controls based on the security categorization, as covered in the previous step. This course also discusses the process for modifying and supplementing the security control baseline based on risk assessment and local conditions. |
| **COURSE PREREQUISITE(S):** None |
| **DAI:** Process Code: IHC04 - Training |

| CS104.16 |
| --- |
| **Risk Management Framework (RMF) Step 3: Implementing Security Controls** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 0.6 hr. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br><br>• Implement the security controls specified in the security plan<br>• Document security control implementation in the security plan |
| **DESCRIPTION:** This course builds on the security controls selected in the previous step of the Risk Management Framework (RMF) process and discusses the implementation of the approved security plan. Upon completion, students will have an understanding of the documentation requirements for security controls, the development of required artifacts, and the process for applying industry best practices to reduce the overall level of risk. |
| **COURSE PREREQUISITE(S):** None |
| **DAI:** Process Code: IHC04 - Training |

| CS105.16 |
| --- |
| **Risk Management Framework (RMF) Step 4: Assessing Security Controls** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 0.5 hr. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br><br>• Explain how to develop and approve a security assessment plan<br>• Assess security controls based on the plan<br>• Identify security assessment results<br>• Describe how to conduct remediation activities |
| **DESCRIPTION:** This course covers the procedures for assessing security controls to ensure they were implemented correctly, operate as intended, and successfully meet the security requirements for the information system. Students will learn how to create a security assessment plan and remediate any remaining deficiencies. |
| **COURSE PREREQUISITE(S):** None |

| |
|---|
| **DAI:** Process Code: IHC04 - Training |

| **CS106.16** |
|---|
| **Risk Management Framework (RMF) Step 5: Authorizing Systems** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 0.5 hr. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br><br>• Prepare a POA&M<br>• Assemble and submit the security authorization package to the Authorizing Official<br>• Recognize and describe the overall risk based on artifacts submitted<br>• Define key resources to make a risk acceptance decision |
| **DESCRIPTION:** This course covers the roles and responsibilities of key stakeholders as they relate to completing, submitting, and approving system authorization packages. This course explores the authorization process from the perspectives of both the system owner and the Authorizing Official, including development of a Plan of Actions and Milestones (POA&M) and the cognizant acceptance of risk. |
| **COURSE PREREQUISITE(S):** None |
| **DAI:** Process Code: IHC04 - Training |

| CS107.16 |
| --- |
| **Risk Management Framework (RMF) Step 6: Monitor Security Controls** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 0.75 hr. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br>• Explain the importance of documenting system changes<br>• Recognize the need for ongoing assessment, risk determination, and remediation<br>• Describe how assessor results can be used<br>• Define the required frequency for reassessment<br>• Explain why status reporting is necessary<br>• Describe the information system removal and disposal process |
| **DESCRIPTION:** This course covers the final step of the Risk Management Framework process: Monitor Security Controls. This step is critical in maintaining an effective security posture and accreditation status. The course modules will prepare the student to for their role and responsibility in reassessing risk and reporting the current status throughout the system lifecycle. |
| **COURSE PREREQUISITE(S):** None |
| **DAI:** Process Code: IHC04 - Training |

| IS123.16 |
| --- |
| **Acquisition and Contracting Basics in the NISP** |
| **SOURCE:** Center for Development of Security Excellence (CDSE) |
| **TMS CODE:** N/A |
| **LOCATION:** CDSE online course |
| **LENGTH:** 1.5 hrs. This is a nonresident, self-paced course available online. |
| **OBJECTIVE:** Trainees who successfully complete this course will be able to:<br>• Identify the phases in the acquisition life cycle<br>• Identify the roles of security professionals in the DoD contracting process<br>• Identify the importance of planning for security across the acquisition life cycle and during the contracting process<br>• Identify the phases of contract administration and the impact of security requirements in the contracting process<br>• Identify the purpose of the security-related contractual documents: DD Form 254, DD Form 441,SF 328<br>• Identify the relationship of the Statement of Work (SOW) or Performance Work Statement (PWS) to DD Form 254 |
| **DESCRIPTION:** This course provides students with a high level overview of acquisitions and contracting basics, including the acquisition life cycle, security requirements and guidance, contract administration, security-related contractual documents, and the fundamental NISP roles and responsibilities. |
| **COURSE PREREQUISITE(S):** None |
| **COURSE COMPLETION REQUIREMENTS**: Completion of an end-of-module test with a 75% score. |
| **DAI:** Process Code: IHC04 - Training |

| CDM Module 1 |
| --- |
| **Continuous Diagnostics and Mitigation (CDM) Module 1 : Overview** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 2 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help the student better understand how CDM can help a D/A better manage risk and protect mission critical assets and to more effectively evaluate their cyber posture. |
| **DESCRIPTION:** This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding Continuous Diagnostics and Mitigation (CDM). The course provides a high level overview of the CDM program. Topics covered include basic CDM concepts, how CDM relates to NIST 800-53 and other NIST SPs, CDM Concept of Operations, the CDM Environment, and CDM's Phases and Capabilities. |
| **DAI:** Process code: IHC04 - Training |

| CDM Module 2 |
| --- |
| **Continuous Diagnostics and Mitigation (CDM) Module 2: Hardware Asset Management (HWAM)** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 1 hr. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help the student better understand how people and devices work together to protect mission critical assets and to more effectively evaluate their cyber posture. |
| **DESCRIPTION:** This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding Continuous Diagnostics and Mitigation (CDM). The course begins by defining HWAM and why it is critical to the implementation of a robust cybersecurity program. The training highlights the criteria for monitoring and managing hardware assets using CDM. It then transitions into HWAM implementation criteria and discusses the generic CDM concept of operations specific to HWAM. Topics covered include Actual State, Desired State, and Defects. |
| **DAI:** Process code: IHC04 - Training |

| CDM Module 3 |
| --- |
| **Continuous Diagnostics and Mitigation (CDM) Module 3: Software Asset Management (SWAM)** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 1.5 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help the student better understand how people and software work together to protect mission critical assets and to more effectively evaluate their cyber posture. |
| **DESCRIPTION:** This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding Continuous Diagnostics and Mitigation (CDM). The course begins by defining SWAM and why it is critical to the implementation of a robust cybersecurity program. It covers new roles and responsibilities which the department or agency (D/A) must implement. It then transitions into SWAM implementation criteria, and discusses the generic CDM concept of operations specific to SWAM Actual State, Desired State, and Defects. It includes high-level discussions of software lists (white, gray, black) and how software can be identified and tracked in CDM through the use of Common Platform Enumeration (CPE) and Software Identification (SWID) tags by Software package down to executables. |
| **DAI:** Process code: IHC04 - Training |

| CDM Module 4 |
| --- |
| **Continuous Diagnostics and Mitigation (CDM) Module 4: Configuration Settings Management** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** .5 hr. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help the student better understand CSM, provide organization visibility into risks associated with improper or non-compliant security-related configuration settings for authorized hardware and software. |
| **DESCRIPTION:** This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding Continuous Diagnostics and Mitigation (CDM). The course begins by outlining CSM and highlighting the types of attacks CSM can help prevent. It then transitions into CSM methods and criteria, where it reviews Actual State, Desired State, and Defect Checks specific to the capability area. It explains how CSM builds upon the other capabilities and how defect checks differ at the local and federal levels. |

| |
|---|
| **DAI:** Process code: IHC04 - Training |

| **CDM Module 5** |
|---|
| **Continuous Diagnostics and Mitigation (CDM) Module 5: Vulnerability Management** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** .5 hr. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help the student better understand how VULN identifies the existence of vulnerable software products in the boundary to allow an organization to mitigate and thwart common attacks that exploit those vulnerabilities. |
| **DESCRIPTION:** The course begins by defining VULN, how it applies to the target environment, and how a fully implemented VULN capability impacts a Department or Agency. It then transitions into VULN criteria and methods, where it reviews Actual State, Desired State, and Defect Checks specific to the capability area. It explains how VULN builds upon the other capabilities areas, the types of defects, and how those defect checks differ at the local and federal levels. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **Cyber Risk Management for Managers** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 6 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to provide an overview of key concepts, issues, and considerations for managing risk from a manager's perspective. |
| **DESCRIPTION:** The course includes discussions identifying critical assets and operations, a primer on cyber threats and how to determine threats to your business function, mitigation strategies, and response and recovery. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **Cyber Security Overview for Managers** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 6 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help managers better understand how people and devices work together to protect mission critical assets and more effectively evaluate their cyber posture. |
| **DESCRIPTION:** The course is designed for managers and other stakeholders who may be involved in decision making regarding their cyber environment but do not have a strong technical background. Discussions will not focus on specific technologies or implementation techniques, but rather cyber security methodologies and the framework for providing a resilient cyber presence. |
| **DAI:** Process code: IHC04 - Training |



| |
|---|
| **DNSSEC Training Workshop** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 2 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help managers better understand how the Domain Name System (DNS) works from the operating system all the way through the authoritative name servers and more effectively evaluate their cyber posture. |
| **DESCRIPTION:** This course covers the basics of DNSSEC, how it integrates into the existing global DNS and provides a step-by-step process to deploying DNSSEC on existing DNS zones. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **Introduction to Investigation of Digital Assets** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 4 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to provide an overview of the digital investigation process and key activities performed throughout the process and various tools that can be used to perform each activity. |
| **DESCRIPTION:** This course covers the basics of DNSSEC, how it integrates into the existing global DNS and provides a step-by-step process to deploying DNSSEC on existing DNS zones. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **Introduction to Windows Scripting** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 4 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to present the basics of Windows BATCH scripting syntax and structure, along with several Windows command line utilities to harness the powerful capabilities built into Windows. |
| **DESCRIPTION:** This course covers the basics of writing scripts for the Microsoft Windows operating system. It covers fundamentals and syntax for automating administrative and security monitoring tasks. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **LAN Security Using Switch Features** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 2 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to provide an overview of the different methods of how to secure Local Area Networks (LANs) at the connectivity level. |
| **DESCRIPTION:** This course covers the basics of monitoring MAC addresses and port security, limiting MAC & IP spoofing, controlling traffic flows, implementing and enhancing security in VLANs, enabling authentication on connection points, and determining host security health. Examples are used throughout the course to reinforce concepts. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **Network Layer 1 & 2 Troubleshooting** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 3 hrs. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to provide a review of troubleshooting methods used in Layer 1 and Layer 2 of the OSI Model. |
| **DESCRIPTION:** The course covers how to detect, trace, identify, and fix network connectivity issues at the Physical and Data Link layers of the OSI stack. The basics of the Physical and Data Link layers will be covered along with a review of the devices, signaling, and cabling which operate at these layers. Students will be presented with methods for tracing connectivity issues back to the source and identifying mitigation solutions. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **Radio Frequency Identification (RFID) Security** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 1 hr. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to provide methods on securing radio frequency identification (RFID). |
| **DESCRIPTION:** The course covers different components of RFID, how it works, applications in which it is being used, benefits and weaknesses, and the communication range over which it works. Students will learn specific concerns with RFID, recommendations for RFID, and security issues that have come to light. |
| **DAI:** Process code: IHC04 - Training |

| |
|---|
| **Securing Infrastructure Devices** |
| **SOURCE:** Federal Virtual Training Environment (FedVTE) |
| **TMS CODE:** N/A |
| **LOCATION:** FedVTE online course |
| **LENGTH:** 1 hr. This is a nonresident, self-paced course available on-line. |
| **OBJECTIVE:** The course aims to help managers better understand how to secure infrastructure devices and more effectively evaluate their cyber posture. |
| **DESCRIPTION:** This course covers physical security, operating system security, management traffic security, device service hardening, securing management services and device access privileges. |
| **DAI:** Process code: IHC04 - Training |

Appendix C. Cybersecurity Shield of Excellence Certificate Request

## CYBERSECURITY SHIELD OF EXCELLENCE CERTIFICATE REQUEST

**(Submit completed form to Software Division Training Coordinator)**

Applicant Name:

First-Line Supervisor:

CMO Name and Organization Code:

Name of CMO Commander/Director:

Command's mailing address:

Software Division Disposition:

Reviewer sign and indicate approval or disapproval as follows:

☐ The package has been reviewed and the individual named is hereby certified.

☐ The package is missing the following information and was not approved.

Sofware Division Reviewer and date of review:

The individual named above has completed 40 hours of training time, which includes the three DAU courses, required by the Cybersecurity Awareness Training Program. (Individual making request must attach a copy of the certificates for each of the courses as substantiating evidence that the course was completed).

DAU courses: (note that an official DAU transcript is sufficient)

- ☐ ACQ160 (Program Protection Plan) (17 hrs)
- ☐ CLE074 (Cybersecurity Throughout DoD Acquisition) (5 hrs)
- ☐ CLE075 (Introduction to DoD Cloud Computing) (4 hrs)

CDSE courses:

- ☐ Introduction to the NISP Certification and Accreditation Process (IS100.16) (2 hrs)
- ☐ Risk Management Framework (RMF) Step 1: Categorization of the System (CS102.16) (0.6 hr)
- ☐ Risk Management Framework (RMF) Step 2: Selecting Security Controls (CS103.16) (0.5 hr)
- ☐ Risk Management Framework (RMF) Step 3: Implementing Security Controls (CS104.16) (0.6 hr)
- ☐ Risk Management Framework (RMF) Step 4: Assessing Security Controls (CS105.16) (0.5 hr)
- ☐ Risk Management Framework (RMF) Step 5: Authorizing Systems (CS106.16) (0.5 hr)
- ☐ Risk Management Framework (RMF) Step 6: Monitor Security Controls (CS107.16)
- ☐ Acquisition and Contracting Basics in the NISP (IS123.16) (0.75 hr)

FedVTE courses:

- ☐ Continuous Diagnostics and Mitigation (CDM) Module 1 : Overview (2 hrs)
- ☐ Continuous Diagnostics and Mitigation (CDM) Module 2: Hardware Asset Management (1 hr)
- ☐ Continuous Diagnostics and Mitigation (CDM) Module 3: Software Asset Management (1.5 hrs)
- ☐ Continuous Diagnostics and Mitigation (CDM) Module 4: Configuration Settings Management (0.5 hr)
- ☐ Continuous Diagnostics and Mitigation (CDM) Module 5: Vulnerability Management (0.5 hr)
- ☐ Cyber Risk Management for Managers (6 hrs)
- ☐ Cyber Security Overview for Managers (6 hrs)
- ☐ DNSSEC Training Workshop (2 hrs)
- ☐ Introduction to Investigation of Digital Assets (4 hrs)
- ☐ Introduction to Windows Scripting (4 hrs)
- ☐ LAN Security Using Switch Features (2 hrs)
- ☐ Network Layer 1 & 2 Troubleshooting (3 hrs)
- ☐ Radio Frequency Identification (RFID) Security (1 hr)
- ☐ Securing Infrastructure Devices (1 hr)

# Appendix B

## Sample Size Calculator[76]

Qualtrics offers a sample-size calculator that can help you determine your ideal sample size in seconds. Just put in the confidence level, population size, margin of error, and the perfect sample size is calculated for you.

**Confidence Level:**

90% ▾

**Population Size:**

500

**Margin of Error:**

10% ▾

**Ideal Sample Size:**

60

### CONFIDENCE INTERVAL

The confidence interval is the plus-or-minus figure that represents the accuracy of the reported. Consider the following example:

A Canadian national sample showed "Who Canadians spend their money on for Mother's Day." Eighty-two percent of Canadians expect to buy gifts for their mom, compared to 20 percent for their wife and 15 percent for their mother-in-law. In terms of spending, Canadians expect to spend $93 on their wife this Mother's Day versus $58 on their mother. The national findings are accurate, plus or minus 2.75 percent, 19 times out of 20.

For example, if you use a confidence interval of 2.75 and 82% percent of your sample indicates they will "buy a gift for mom" you can be "confident (95% or 99%)" that if you had asked the question to ALL CANADIANS, somewhere between 79.25% (82%-2.75%) and 84.75% (82%+2.75%) would have picked that answer.

### CONFIDENCE LEVEL

The confidence level tells you how confident you are of this result. It is expressed as a percentage of times that different samples (if repeated samples were drawn) would produce this result. The 95% confidence level means that 19 times out of twenty that results would fall in this – + interval confidence interval. The 95% confidence level is the most commonly used.

When you put the confidence level and the confidence interval together, you can say that you are 95% (19 out of 20) sure that the true percentage of the population that will "buy a gift for mom" is between 79.25% and 84.75%.

Wider confidence intervals increase the certainty that the true answer is within the range specified. These wider confidence intervals come from smaller sample sizes. When the costs of an error is extremely high (a multi-million dollar decision is at stake) the confidence interval should be kept small. This can be done by increasing the sample size.

## Notes

[1] United States Government Accountability Office. *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements: Report to Congressional Committees*. Washington, D.C.: United States Government Accountability Office, 2011. http://purl.fdlp.gov/GPO/gpo13750.

[2] Reilly, Jeffrey M. "Multidomain Operations: A Subtle but Significant Transition in Military Thought." *Air & Space Power Journal* 30, no. 1 (Spring 2016), 61-73.

[3] Ross, Ron, Patrick Viscuso, Gary Guissanie, Kelley Dempsey; Dempsey, and Mark Riddle. *NIST SP 800-171 Rev. 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology, 2017.

[4] Gallagher, Patrick D. *NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology, 2013.

[5] Ross, Ron, Patrick Viscuso, Gary Guissanie, Kelley Dempsey; Dempsey, and Mark Riddle. *NIST SP 800-171 Rev. 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology, 2017.

[6] Kozloski, Matt. "Everything You Need to Know About NIST 800-171." The Kelser Blog. Last modified December 16, 2016. https://inbound.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171.

[7] CyberDefenses Inc. "NIST SP 800-171." CyberDefenses Inc. Last modified 2017. https://cyberdefenses.com/nist-sp-800-171/.

[8] Harris, Shon, and Fernando Maymí. *CISSP All-in-One Exam Guide*, 7th ed. New York: McGraw-Hill, 2016.

[9] Ibid.

[10] Ibid.

[11] Ross, Ron, Patrick Viscuso, Gary Guissanie, Kelley Dempsey; Dempsey, and Mark Riddle. *NIST SP 800-171 Rev. 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology, 2017; Kozloski, Matt. "Everything You Need to Know About NIST 800-171." The Kelser Blog. Last modified December 16, 2016. https://inbound.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171

[12] Assad, Shay D. *Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*. Washington, DC: Defense Pricing/Defense Procurement and Acquisition Policy, 2017.

[13] Clausen, Christian. "The importance of cybersecurity." *Aerotech News and Review* (Lancaster, CA), November 4, 2016. http://www.aerotechnews.com/nellisafb/2016/11/04/the-importance-of-cybersecurity/.

[14] Garamone, Jim. "Cyber Tops List of Threats to U.S., Director of National Intelligence." U.S. Department of Defense. Last modified February 13, 2018. https://www.defense.gov/News/Article/Article/1440838/.

[15] Defense Contract Management Agency. "DCMA Announces New Mission Statement." *Defense Contract Management Agency*, 25 Sept. 2014, www.dcma.mil/News/Article-View/Article/815360/dcma-announces-new-mission-statement/.

[16] Defense Contract Management Agency. DCMA-INST 203. *Software Acquisition Management.* 25 June 2013.

[17] Information Assurance Training Center. "DoD Cyber Awareness Challenge Training." US Army Cyber Center of Excellence. Last modified 2018. https://ia.signal.army.mil/dodiaa/.

[18] Defense Contract Management Agency. "Instructions for Cyber Awareness Challenge-Information Assurance Training." DCMA Learn Center. Last modified 2015. https://dcma.usalearning.net/course/view.php?id=180.

[19] Gutierrez, Karla. "A Quick Overview of Four Instructional Design Models." SHIFT E-Learning Software. Last modified August 25, 2015. https://www.shiftelearning.com/blog/top-instructional-design-models-explained.

[20] Allen, W. C. "Overview and Evolution of the ADDIE Training System." *Advances in Developing Human Resources* 8, no. 4 (November 2006), 430-441.

[21] Ibid.

[22] Ibid.

[23] Rimmer, Trina. "An Introduction to SAM for Instructional Designers." E-Learning Heroes. Last modified November 2016. https://community.articulate.com/articles/an-introduction-to-sam-for-instructional-designers.

[24] Huhn, Jake. "Agile Vs ADDIE: Which Is Better for Learning Design?" ELearning Learning. Last modified May 11, 2013. http://www.elearninglearning.com/addie/agile/?open-article-id=2043492&article-title=agile-vs-addie--which-is-better-for-learning-design-&blog-domain=bottomlineperformance.com&blog-title=bottom-line-performance.

[25] Pappas, Christopher. "The Power of AGILE Instructional Design Approach." ELearning Industry. Last modified April 19, 2015. https://elearningindustry.com/the-power-of-agile-instructional-design-approach.

[26] Ibid.

[27] Huhn, Jake. "What Is Agile Learning Design?" ELearning Learning. Last modified May 7, 2013. http://www.elearninglearning.com/addie/agile/?open-article-id=2033688&article-title=what-is-agile-learning-design-&blog-domain=bottomlineperformance.com&blog-title=bottom-line-performance.

[28] Allen, Michael W., and Richard Sites. *Leaving ADDIE for SAM: An Agile Model for Developing the Best Learning Experiences*. Alexandria, VA: ASTD Press, 2012.

[29] Ibid.

[30] Pappas, Christopher. "Top 7 Instructional Design Theories & Models for Your Next ELearning Course." ELearning Industry. Last modified September 2, 2017. https://elearningindustry.com/top-instructional-design-theories-models-next-elearning-course.

[31] Rimmer, Trina. "An Introduction to SAM for Instructional Designers." E-Learning Heroes. Last modified November 2016. https://community.articulate.com/articles/an-introduction-to-sam-for-instructional-designers.

[32] Ibid.

[33] Culatta, Richard. " Weaknesses of the ADDIE Model." Instructional Design. Last modified 2013. http://www.instructionaldesign.org/models/addie_weaknesses.html.

[34] Ibid.

[35] Castagnolo, Chuck. "The Addie Model: Why Use It?" THE ELearning Site. Last modified March 1, 2011. http://theelearningsite.com/2011/03/the-addie-model-why-use-it/.

[36] Sincero, Sarah M. "Advantages and Disadvantages of Surveys." Explorable. Last modified March 18, 2012. https://explorable.com/advantages-and-disadvantages-of-surveys; Debois, Stefan. "9 Advantages and Disadvantages of Questionnaires." Survey Anyplace. Last modified March 16, 2016. https://surveyanyplace.com/questionnaire-pros-and-cons/.

[37] Sincero, Sarah M. "Advantages and Disadvantages of Surveys." Explorable. Last modified March 18, 2012. https://explorable.com/advantages-and-disadvantages-of-surveys.

[38] Debois, Stefan. "9 Advantages and Disadvantages of Questionnaires." Survey Anyplace. Last modified March 16, 2016. https://surveyanyplace.com/questionnaire-pros-and-cons/.

[39] Blackstone, Amy. *Principles of Sociological Inquiry: Qualitative and Quantitative Methods, v. 1.0*. Boston, MA: FlatWorld, 2018. https://catalog.flatworldknowledge.com/bookhub/reader/3585?e=blackstone_1.0-ch08_s02; Sincero, Sarah M. "Advantages and Disadvantages of Surveys." Explorable. Last modified March 18, 2012. https://explorable.com/advantages-and-disadvantages-of-surveys.

[40] Sincero, Sarah M. "Advantages and Disadvantages of Surveys." Explorable. Last modified March 18, 2012. https://explorable.com/advantages-and-disadvantages-of-surveys.

[41] Desman, Mark B. *Building an Information Security Awareness Program*. Hoboken: Taylor and Francis, 2013.

[42] Wilson, Mark, and Joan Hash. *NIST SP 800-50: Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD: National Institute of Standards and Technology, 2003.

[43] Gardner, Bill, and Valerie Thomas. *Building an Information Security Awareness Program: Defending against Social Engineering and Technical Threats*. Waltham, MA: Elsevier Inc., 2014.

[44] Ibid.

[45] Wilson, Mark, and Joan Hash. *NIST SP 800-50: Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD: National Institute of Standards and Technology, 2003.

[46] Jackson, William. "A Flight Plan for Safer Software." GCN. Last modified February 9, 2009. https://gcn.com/articles/2009/02/09/flight-plan-for-safer-software.aspx.

[47] Kagan, Mark. "Best Practices: ProveIT Case Study for U.S. Air Force Software Assurance Center of Excellence." Federal News Radio- FederalNewsRadio.com. Last modified March 2009. http://federalnewsradio.com/wpcontent/uploads/pdfs/ProveIT.pdf.

[48] Jackson, William. "A Flight Plan for Safer Software." GCN. Last modified February 9, 2009. https://gcn.com/articles/2009/02/09/flight-plan-for-safer-software.aspx.

[49] Jackson, William. "A Flight Plan for Safer Software." GCN. Last modified February 9, 2009. https://gcn.com/articles/2009/02/09/flight-plan-for-safer-software.aspx; Kagan, Mark. "Best Practices: ProveIT Case Study for U.S. Air Force Software Assurance Center of Excellence." Federal News Radio- FederalNewsRadio.com. Last modified March 2009. http://federalnewsradio.com/wpcontent/uploads/pdfs/ProveIT.pdf.

[50] Jackson, William. "A Flight Plan for Safer Software." GCN. Last modified February 9, 2009. https://gcn.com/articles/2009/02/09/flight-plan-for-safer-software.aspx.

[51] Ibid.

[52] Woodworth, James. “Building Assurance into Software Development Life-Cycle (SDLC)”. PowerPoint Presentation, Gunter AFB, AL, 2009.

[53] Jackson, William. "A Flight Plan for Safer Software." GCN. Last modified February 9, 2009. https://gcn.com/articles/2009/02/09/flight-plan-for-safer-software.aspx.

[54] Kagan, Mark. "Best Practices: ProveIT Case Study for U.S. Air Force Software Assurance Center of Excellence." Federal News Radio- FederalNewsRadio.com. Last modified March 2009.

[55] Jackson, William. "A Flight Plan for Safer Software." GCN. Last modified February 9, 2009. https://gcn.com/articles/2009/02/09/flight-plan-for-safer-software.aspx.

[56] Ibid.

[57] James Woodworth in discussion with the author, December 2017.

[58] Ackerman, Robert K. "DISA Takes Proactive Approach to Cyberthreats." SIGNAL Magazine. Last modified April 21, 2016. https://www.afcea.org/content/?q=Article-disa-takes-proactive-approach-cyberthreats.

[59] Ackerman, Robert K. "DISA Takes Proactive Approach to Cyberthreats." SIGNAL Magazine. Last modified April 21, 2016. https://www.afcea.org/content/?q=Article-disa-takes-proactive-approach-cyberthreats.

[60] Ackerman, Robert K. "DISA Takes Proactive Approach to Cyberthreats." SIGNAL Magazine. Last modified April 21, 2016. https://www.afcea.org/content/?q=Article-disa-takes-proactive-approach-cyberthreats.

[61] Betty Linney, e-mail message to author, December 5, 2017.

[62] Benton Tiffiney. “Continuous Cybersecurity Training Program”. PowerPoint Presentation, DISA Headquarters, Fort Meade, April 17, 2017.

[63] Johnson, Nicole B. "DISA Vice Director: 4 Tenets to Educate the Federal Workforce in Cyber." GovLoop. Last modified May 16, 2017. https://www.govloop.com/disa-vice-director-4-tenets-educating-federal-workforce-cyber/.

[64] Benton Tiffiney. “Continuous Cybersecurity Training Program”. PowerPoint Presentation, DISA Headquarters, Fort Meade, April 17, 2017.

[65] Johnson, Nicole B. "DISA Vice Director: 4 Tenets to Educate the Federal Workforce in Cyber." GovLoop. Last modified May 16, 2017. https://www.govloop.com/disa-vice-director-4-tenets-educating-federal-workforce-cyber/.

[66] Benton Tiffiney. “Continuous Cybersecurity Training Program”. PowerPoint Presentation, DISA Headquarters, Fort Meade, April 17, 2017.

[67] Billy Price e-mail message the author, December 2017.

[68] Joseph Zell e-mail message the author, December 2017.

[69] Symantec. "Phishing Readiness." Symantec. Last modified 2017. https://www.symantec.com/products/phishing-readiness.

[70] Joseph Zell e-mail message the author, December 2017.

[71] Symantec. "Security Awareness Service." Symantec. Last modified 2018. https://www.symantec.com/services/education-services/campaigns/security-awareness.

[72] David Fagan e-mail message the author, December 2017.

[73] Nayak, Barun K. "Understanding the relevance of sample size calculation." *Indian Journal of Ophthalmology* 58, no. 6 (November/December 2010), 469-470. doi:10.4103/0301-4738.71673.

[74] Gorman, Carol N. *DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued from August 1, 2015, Through July 31, 2016 (Report No. DODIG-2017-034).* Alexandria, VA: DoD Inspector General, 2016.

[75] Defense Contract Management Agency. *Cybersecurity Awareness Training Program Guide*, 3 March 2017.

[76] Qualtrics. "Sample Size Calculator." Qualtrics. Last modified April 12, 2010. https://www.qualtrics.com/blog/calculating-sample-size/.

# Bibliography


Ackerman, Robert K. "DISA Takes Proactive Approach to Cyberthreats." SIGNAL Magazine. Last modified April 21, 2016. https://www.afcea.org/content/?q=Article-disa-takes-proactive-approach-cyberthreats.

Allen, Michael W., and Richard Sites. *Leaving ADDIE for SAM: An Agile Model for Developing the Best Learning Experiences*. Alexandria, VA: ASTD Press, 2012.

Allen, W. C. "Overview and Evolution of the ADDIE Training System." *Advances in Developing Human Resources* 8, no. 4 (November 2006), 430-441.

Assad, Shay D. *Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*. Washington, DC: Defense Pricing/Defense Procurement and Acquisition Policy, 2017.

Benton Tiffiney. "Continuous Cybersecurity Training Program". PowerPoint Presentation, DISA Headquarters, Fort Meade, April 17, 2017.

Blackstone, Amy. *Principles of Sociological Inquiry: Qualitative and Quantitative Methods, v. 1.0*. Boston, MA: FlatWorld, 2018. https://catalog.flatworldknowledge.com/bookhub/reader/3585?e=blackstone_1.0-ch08_s02.

Castagnolo, Chuck. "The Addie Model: Why Use It?" THE ELearning Site. Last modified March 1, 2011. http://theelearningsite.com/2011/03/the-addie-model-why-use-it/.

Clausen, Christian. "The importance of cybersecurity." *Aerotech News and Review* (Lancaster, CA), November 4, 2016. http://www.aerotechnews.com/nellisafb/2016/11/04/the-importance-of-cybersecurity/.

Culatta, Richard. " Weaknesses of the ADDIE Model." Instructional Design. Last modified 2013. http://www.instructionaldesign.org/models/addie_weaknesses.html.

CyberDefenses Inc. "NIST SP 800-171." CyberDefenses Inc. Last modified 2017. https://cyberdefenses.com/nist-sp-800-171/.

Debois, Stefan. "9 Advantages and Disadvantages of Questionnaires." Survey Anyplace. Last modified March 16, 2016. https://surveyanyplace.com/questionnaire-pros-and-cons/.

Defense Contract Management Agency. *Cybersecurity Awareness Training Program Guide*, 3 March 2017.

Defense Contract Management Agency. *Cybersecurity Awareness Training Evaluation Survey*, 7 March 2017.

Defense Contract Management Agency. DCMA-INST 203. *Software Acquisition Management.* 25 June 2013.

Defense Contract Management Agency. "DCMA Announces New Mission Statement." *Defense Contract Management Agency*, 25 Sept. 2014, www.dcma.mil/News/Article-View/Article/815360/dcma-announces-new-mission-statement/.

Defense Contract Management Agency. "Instructions for Cyber Awareness Challenge-Information Assurance Training." DCMA Learn Center. Last modified 2015. https://dcma.usalearning.net/course/view.php?id=180.

Desman, Mark B. *Building an Information Security Awareness Program*. Hoboken: Taylor and Francis, 2013.

Gallagher, Patrick D. *NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology, 2013.

Garamone, Jim. "Cyber Tops List of Threats to U.S., Director of National Intelligence." U.S. Department of Defense. Last modified February 13, 2018. https://www.defense.gov/News/Article/Article/1440838/.

Gardner, Bill, and Valerie Thomas. *Building an Information Security Awareness Program: Defending against Social Engineering and Technical Threats*. Waltham, MA: Elsevier Inc., 2014.

Gorman, Carol N. *DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued from August 1, 2015, Through July 31, 2016 (Report No. DODIG-2017-034)*. Alexandria, VA: DoD Inspector General, 2016.

Gutierrez, Karla. "A Quick Overview of Four Instructional Design Models." SHIFT E-Learning Software. Last modified August 25, 2015. https://www.shiftelearning.com/blog/top-instructional-design-models-explained.

Harris, Shon, and Fernando Maymí. *CISSP All-in-One Exam Guide*, 7th ed. New York: McGraw-Hill, 2016.

Huhn, Jake. "Agile Vs ADDIE: Which Is Better for Learning Design?" ELearning Learning. Last modified May 11, 2013. http://www.elearninglearning.com/addie/agile/?open-article-id=2043492&article-title=agile-vs-addie--which-is-better-for-learning-design-&blog-domain=bottomlineperformance.com&blog-title=bottom-line-performance.

Huhn, Jake. "What Is Agile Learning Design?" ELearning Learning. Last modified May 7, 2013.

http://www.elearninglearning.com/addie/agile/?open-article-id=2033688&article-title=what-is-agile-learning-design-&blog-domain=bottomlineperformance.com&blog-title=bottom-line-performance.

Information Assurance Training Center. "DoD Cyber Awareness Challenge Training." US Army Cyber Center of Excellence. Last modified 2018. https://ia.signal.army.mil/dodiaa/.

Jackson, William. "A Flight Plan for Safer Software." GCN. Last modified February 9, 2009. https://gcn.com/articles/2009/02/09/flight-plan-for-safer-software.aspx.

Johnson, Nicole B. "DISA Vice Director: 4 Tenets to Educate the Federal Workforce in Cyber." GovLoop. Last modified May 16, 2017. https://www.govloop.com/disa-vice-director-4-tenets-educating-federal-workforce-cyber/.

Kagan, Mark. "Best Practices: ProveIT Case Study for U.S. Air Force Software Assurance Center of Excellence." Federal News Radio- FederalNewsRadio.com. Last modified March 2009.

Kozloski, Matt. "Everything You Need to Know About NIST 800-171." The Kelser Blog. Last modified December 16, 2016. https://inbound.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171.

Nayak, Barun K. "Understanding the relevance of sample size calculation." *Indian Journal of Ophthalmology* 58, no. 6 (November/December 2010), 469-470. doi:10.4103/0301-4738.71673.

Pappas, Christopher. "The Power of AGILE Instructional Design Approach." ELearning Industry. Last modified April 19, 2015. https://elearningindustry.com/the-power-of-agile-instructional-design-approach.

Pappas, Christopher. "Top 7 Instructional Design Theories & Models for Your Next ELearning Course." ELearning Industry. Last modified September 2, 2017. https://elearningindustry.com/top-instructional-design-theories-models-next-elearning-course.

Qualtrics. "Sample Size Calculator." Qualtrics. Last modified April 12, 2010. https://www.qualtrics.com/blog/calculating-sample-size/.

Reilly, Jeffrey M. "Multidomain Operations: A Subtle but Significant Transition in Military Thought." *Air & Space Power Journal* 30, no. 1 (Spring 2016), 61-73.

Rimmer, Trina. "An Introduction to SAM for Instructional Designers." E-Learning Heroes. Last modified November 2016. https://community.articulate.com/articles/an-introduction-to-sam-for-instructional-designers.

Ross, Ron, Patrick Viscuso, Gary Guissanie, Kelley Dempsey; Dempsey, and Mark Riddle. *NIST*

*SP 800-171 Rev. 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Gaithersburg, MD: National Institute of Standards and Technology, 2017.

Sincero, Sarah M. "Advantages and Disadvantages of Surveys." Explorable. Last modified March 18, 2012. https://explorable.com/advantages-and-disadvantages-of-surveys.

Symantec. "Phishing Readiness." Symantec. Last modified 2017. https://www.symantec.com/products/phishing-readiness.

Symantec. "Security Awareness Service." Symantec. Last modified 2018. https://www.symantec.com/services/education-services/campaigns/security-awareness.

United States Government Accountability Office. *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements: Report to Congressional Committees*. Washington, D.C.: United States Government Accountability Office, 2011. http://purl.fdlp.gov/GPO/gpo13750.

Wilson, Mark, and Joan Hash. *NIST SP 800-50: Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD: National Institute of Standards and Technology, 2003.

Woodworth, James. "Building Assurance into Software Development Life-Cycle (SDLC)". PowerPoint Presentation, Gunter AFB, AL, 2009.